

REMARKS

No claims are currently amended. Claims 4-5, 14-15, 21-22, 26, and 29 were previously canceled. Claims 1-3, 6-13, 16-20, 23-25, 27-28, and 30-33 are pending and are listed below. In view of the following remarks, Applicant respectfully requests that this application be allowed and forwarded on to issuance.

§103(a) Rejections

Claims 1-3, 6-13, 16-18, 20, 23-25, 27-28, and 33 stand rejected under 35 U.S.C. §103(a) as being anticipated by U.S. Patent No. 6,199,204 to Donohue (hereinafter, "Donohue") in view of U.S. Patent No. 7,000,247 to Banzhof (hereinafter, "Banzhof"). Applicant respectfully traverses the rejections.

Claim 1 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature at a server computing device;
- receiving a security patch at the server computing device;
- identifying, from the server computing device, a vulnerable binary file located on a client computing device based on the binary signature, the client computing device being remote from the server computing device; and
- *updating, from the server computing device, the vulnerable binary file located on the client computing device* with the security patch.

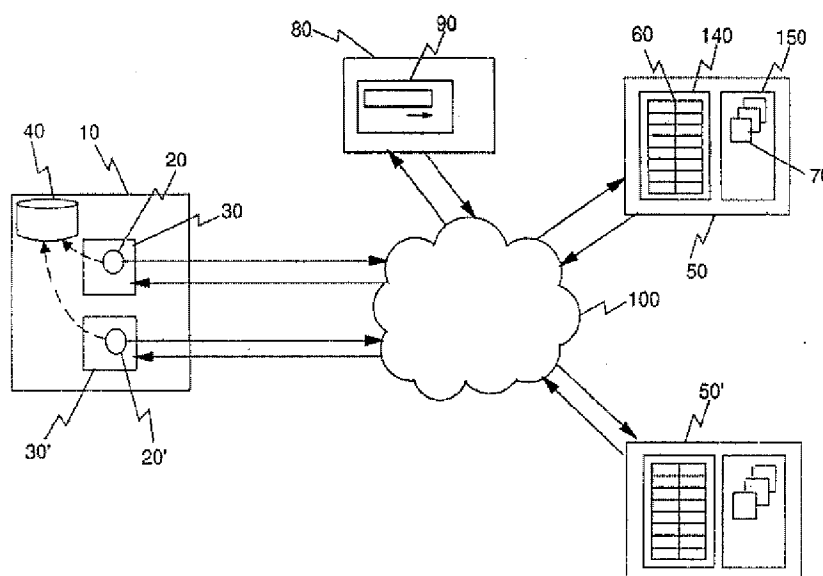
Applicant respectfully submits that the Office fails, in current Action, to state a *prima facie* case of anticipation, as the Office fails to show how the cited references teach or suggest each of Applicant's claim elements. For instance,

Applicant submits that the Office at least fails to show how the cited references teach or suggest “updating, *from the server computing device*, the vulnerable binary file located on the client computing device”. In fact, Applicant respectfully submits that the Office admits as much.

In making out a rejection of claim 1, the Office cites to Donohue as teaching “receiving a binary signature”, “receiving a security patch”, “identifying a vulnerable file”, and “updating” the vulnerable file with the security patch. The Office, however, concedes that “Donohue doesn’t expressly disclose receiving the binary signature at the server computing device as well as the security patch and identifying from the server device the vulnerable binary file and then updating from the server device the vulnerable file on the client”. *Office Action mailed 04/18/2007*, p. 3. Applicant agrees that Donohue discloses no such teaching. The Office continues, however, and states that “Donohue does however disclose an updater component on a network which updates the file [on] other computers on the network”. *Id.* The Office then cites to Banzhof for teaching “receiving binary signatures” and “identifying vulnerable files”. *Id.*

Applicant respectfully submits that the Office fails to state a *prima facie* case of obviousness by failing to show how the cited references teach or suggest “updating, *from the server computing device*, the vulnerable binary file located on the client computing device”. Applicant bases this argument on at least the following two reasons: (1) while the Office cites Donohue’s updater component to apparently remedy the Office’s admission that Donohue does not update from a server computing device, this updater component resides on a client and not a server, and (2) the Office does not cite to Banzhof as teaching this claim element.

First, Applicant respectfully submits that the Office's citation of Donohue's updater component fails to overcome the Office's concession that Donohue does not update from a server computing device. To appreciate this fact, an understanding of the Donohue disclosure is necessary. Donohue describes an updater agent that is *associated with a computer program on a client computer* and that accesses relevant network locations to download and install updates to *the agent's associated program on the client computer*. The agent downloads and installs the updates if those updates satisfy predefined update criteria of the updater agent. *Donohue*, abstract. As Donohue's Fig. 1 illustrates, the updater component 20 is installed in system memory of a conventional network-connected computer system 10 and functions to perform updates on that computer. *Id.* at col. 6, lines 3-6.



As Donohue's text and foregoing illustrate make clear, Donohue's updater agent both resides on a computer and makes updates to that computer. As such, Donohue fails to teach or suggest "updating, from the server computing device, the

vulnerable binary file located on the client computing device", as recited in Applicant's claim. (emphasis added).

Additionally, the Office does not cite to Banzhof as teaching this element. As such, Applicant respectfully submits that the Office's citation of Banzhof fails to remedy the impropriety in the rejection of claim 1.

For at least these reasons, Applicant respectfully submits that this claim stands allowable.

Claims 2-3 and 6-7 depend from claim 1 and, as such, the remarks made above in regards to claim 1 apply equally to these claims. The rejections of these claims are also improper as failing to show how the references of record teach or suggest, either singly or in combination, these claims' own recited features in combination with those recited in claim 1.

Claim 8 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature that identifies a security vulnerability in a binary file;
- receiving a security patch configured to fix the security vulnerability in the binary file; and
- *distributing the binary signature and the security patch to a plurality of servers.*

In making out a rejection of this claim, the Office initially appears to reject this claim under §103(a) in view of Donohue and Banzhof. In the substance of the Action, however, the Office then states that Donohue anticipates this claim. Regardless of the form of the Office's rejection, Applicant respectfully submits

that the Office fails to show how Donohue and/or Banzhof disclose, teach, or suggest Applicant's claim, either alone or in combination.

Specifically, Applicant respectfully submits that the Office fails to show how Donohue or Banzhof discloses "distributing [a] binary signature and [a] security patch to a plurality of servers", as recited in Applicant's claim. In stating that Donohue discloses this element, the Office appears to chiefly rely on Donohue's column seven, lines 55-65. Applicant reproduces this passage for the Office's convenience:

The system 10 of FIG. 1 is shown connected within a network 100 of computers including a number of remote server systems (50,50') from which software resources are available for applying updates to programs installed on the local system 10. Each server system includes within storage a list 60 of the latest versions of, and patches for, software products which are available from that server. Each vendor is assumed here to make available via their Web sites such a list 60 of software updates (an example of which is shown in FIG. 2) comprising their product release history, in a format which is readable by updater components...

Donohue, col. 7, lines 55-65 (emphasis added).

Applicant submits that the above passage merely discusses a network 100 that includes multiple remote server systems, with each server containing a list 60 of the latest versions, and patches for, software products available from that particular server. In other words, this passage merely states that each server within the network contains updates and patches for whatever software product the server is associated with. Donohue's updater agent may then access the relevant server and download the server's list of updates.

First, Applicant respectfully submits that this passage fails to disclose "distributing [a] binary signature and [a] security patch to a plurality of servers".

Instead, this passage merely states that each server in the network *contains* a list of updates. Furthermore, the updater agent on a computer goes out and obtains this list—but Donohue does not disclose distributing that list to a plurality of other servers.

Furthermore, Applicant submits that each server within the Donohue network 100 appears to correspond to different software products. Each server thus contains a list of updates and patches for a particular software product. As such, each server contains *different* updates and patches. Therefore, even assuming that “each vendor” distributes these updates and patches to a corresponding server, not a single vendor has been shown to distribute these updates and patches to a “plurality of servers”. The cited portion of Donohue therefore fails to disclose “distributing *the* binary signature and *the* security patch to a plurality of servers”, as recited in Applicant’s claim. (emphasis added). Applicant further notes that this claim does not merely recite distributing *any sort of* binary signature and security patch, but rather recites distributing *the* received binary signature and *the* received security patch to a plurality of servers—and not to a single corresponding server.

For at least this reason, this claim stands allowable.

Claims 9 and 10 depend from claim 8 and, as such, the remarks made above in regards to claim 8 apply equally to these claims. The rejections of these claims are also improper as failing to show how the references of record teach or suggest, either singly or in combination, these claims’ own recited features in combination with those recited in claim 8.

Claim 11 recites a processor-readable medium having a tangible component and comprising processor-executable instructions configured for (emphasis added):

- receiving a binary signature from a server;
- searching for the binary signature in binary files located on a client computer;
- *sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature*;
- receiving the security patch from the server; and
- updating on the client computer the binary file with the security patch..

In making out a rejection of this claim, the Office again initially appears to reject this claim under §103(a) in view of Donohue and Banzhof. In the substance of the Action, however, the Office then states that Donohue anticipates. Regardless of the form of the Office's rejection, Applicant respectfully submits that the Office fails to show how Donohue and/or Banzhof disclose, teach, or suggest Applicant's claim, either alone or in combination.

Applicant respectfully submits that the Office at least fails to show how Donohue or Banzhof discloses "*sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature*", as recited in Applicant's claim. (emphasis added). In this regard, Applicant submits that: (1) the cited portion of Donohue fails to disclose this claim element, and (2) Donohue as a whole fails to disclose this element.

First, Applicant submits that the cited portion of Donohue fails to disclose this claim element. In stating that Donohue does indeed anticipate this element,

the Office cites to Donohue's column 13, lines 6-10. Applicant reproduces this passage, as well as some surrounding text, for the Office's convenience:

Structure of Updater Component

The structure of an updater component comprises data, methods for operating on that data, and a public application programming interface (API) which allows other updater components to contact and communicate with it. ***This structure will now be described in detail.***

* * *

Receive_Event(event details)

When an updater component receives a request to update, it must inform the calling updater component when it has completed the update or otherwise e.g. if it failed for some reason. The updater component performing the update on behalf of another updater component will call this function of the requesting updater component to communicate success of the update or otherwise.

Donohue, col. 11, lines 20-25, col. 13, lines 5-13 (emphasis added).

As the first of the two passages explains, the second and cited Donohue passage relates to the *structure of the updater component that resides on a conventional computer*. With this context in mind, the cited passage then explains that a first "updater component [may] receive[] a request to update" from another "calling updater agent". As discussed in portions of Donohue following this passage, the cited passage relates to multiple updater components for differing associated computer programs communicating with one another. As Donohue describes, an updater component associated with a first software program may recognize that another second software program is a pre-requisite to updating the first software program. This first updater component may then "call" an updater

component associated with the second computer program and request that the latter updater component update the second computer program. *Id.* at col. 13, lines 22-54. Applicant submits that cited passage of Donohue merely relates to this interrelationship between multiple updater components residing on a same conventional computer.

Applicant respectfully submits that this passage—relating to requests *between* updater components, all resident on a single computer—fails to disclose “*sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature*”, as recited in Applicant’s claim. (emphasis added). In fact, Applicant respectfully submits that this cited passage fails to relate to the sending of a request to any sort of server whatsoever. Additionally, the described communication between updater components fails to disclose “request[ing]...a security patch”, as well as sending a request “if a binary file is found that includes the binary signature”. Applicant thus respectfully submits that the Office fails to show how Donohue anticipates Applicant’s claim.

For at least this reason, Applicant respectfully submits that this claim stands allowable.

Secondly, Applicant respectfully submits that Donohue as a whole at least fails to disclose “*sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature*”, as recited in Applicant’s claim. (emphasis added).

As discussed above, Donohue has at most been shown to disclose an updater agent that is associated with a computer program and that *accesses relevant network locations and automatically downloads and installs any available updates to its associated program*. *Donohue*, abstract (emphasis added).

As such, Donohue's updater agent merely retrieves available updates from a network location and automatically installs them on a computer.

Applicant contrasts this Applicant's claim 11, which recites "receiving a binary signature from a server; *searching for the binary signature* in binary files located on a client computer; [and] *sending a request from the client computer to the server for a security patch if a binary file is found that includes the binary signature*". (emphasis added). Donohue's updater agent does not so "receiv[e]..., search[], [and] request[]"—the updater agent merely retrieves the updates and installs them.

For at least this additional reason, this claim stands allowable.

Claim 12 depends from claim 11 and, as such, the remarks made above in regards to claim 11 apply equally to this claim. The rejections of this claim is also improper as failing to show how the references of record teach or suggest, either singly or in combination, this claim's own recited features in combination with those recited in claim 11.

Claim 13 recites a method comprising (emphasis added):

- receiving a binary signature from a server and at a client computer;
- searching on the client computer for a vulnerable file based on the binary signature;
- *if a vulnerable file is found on the client computer, requesting a security patch from the server;*
- receiving the security patch from the server and at the client computer in response to the request for the security patch from the client computer; and
- fixing the vulnerable file with the security patch received from the server.

In making out a rejection of this claim, the Office states that Donohue and Banzhof render this claim obvious for reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that the Office fails to show how Donohue and Banzhof teach or suggest this claim. Namely, Applicant respectfully submits that the Office fails to show how Donohue or Banzhof teach or suggest “if a vulnerable file is found on the client computer, requesting a security patch from the server”, as recited in Applicant’s claim. Instead, the Office at most shows that Donohue retrieves and automatically installs updates to a computer.

For at least this reason, Applicant respectfully submits that this claim stands allowable.

Claims 16-19 depend from claim 13 and, as such, the remarks made above in regards to claim 13 apply equally to these claims. The rejections of these claims are also improper as failing to show how the references of record teach or suggest, either singly or in combination, these claims’ own recited features in combination with those recited in claim 13. In addition, while claim 19 is rejected over the Donohue/Banzhof in further view of U.S. Patent No. 5,930,504 to Gabel (hereinafter, “Gabel”), the Office does not cite Gabel as teaching or suggesting claims elements that the rejection of base claim 13 lacks. This claim thus stands allowable at least for its dependency upon claim 13.

Claim 20 recites method comprising:

- receiving, at a scan/patch server, a binary signature and a security patch from a distribution server;
- searching, by the scan/patch server, on a client computer for a vulnerable file associated with the binary signature; and

- if a vulnerable file is found, fixing, by the scan/patch server, the vulnerable file on the client computer with the security patch.

In making out a rejection of this claim, the Office states that Donohue and Banzhof render the claim obvious, and uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that the Office fails to show how the references teach or suggest this claim. For instance, Applicant respectfully submits that the Office fails to show how Donohue or Banzhof teaches or suggests “receiving, *at a scan/patch server*, a binary signature and a security patch”, “searching, *by the scan/patch server, on a client computer* for a vulnerable file associated with the binary signature”, and “fixing, *by the scan/patch server, the vulnerable file on the client computer*”, as recited in Applicant’s claim. (emphasis added).

For at least these reasons, Applicant respectfully submits that this claim stands allowable.

Claim 23 recites a computer comprising (emphasis added):

- means for receiving, at a client computer, a binary signature from a server;
- means for searching for a vulnerable file located on the client computer based on the binary signature;
- *means for requesting, by the client computer, a security patch from the server if a vulnerable file is found on the client computer;*
- means for receiving the security patch from the server at the client computer responsive to the request for the security patch; and
- means for fixing the vulnerable file with the security patch received from the server.

In making out a rejection of this claim, the Office states that Donohue anticipates and/or that Donohue and Banzhof render the claim obvious. To do so, the Office uses reasoning similar to that discussed above in regards to claim 11. Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that the Office fails to show how Donohue anticipates this claim and, further, that Donohue as a whole fails to so anticipate. Applicant also respectfully submits that the Office fails to show how Donohue and Banzhof, alone or in combination, teach or suggest this claim. Namely, the Office fails to show how Donohue and Banzhof disclose, teach, or suggest, “means for requesting, by the client computer, a security patch from the server if a vulnerable file is found on the client computer”, as recited in Applicant’s claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, Applicant respectfully submits that this claim stands allowable.

Claim 24 recites a server comprising:

- means for receiving, at a scan/patch server, a binary signature and a security patch from a distribution server;
- means for scanning, from the scan/patch server, a client computer for a vulnerable file associated with the binary signature; and
- means for fixing, from the scan/patch server, the vulnerable file on the client computer with the security patch if a vulnerable file is found on the client computer.

In making out a rejection of this claim, the Office states that Donohue anticipates and/or that Donohue and Banzhof render the claim obvious. To do so, the Office uses reasoning similar to that discussed above in regards to claim 11.

Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that the Office fails to show how Donohue anticipates this claim and, further, that Donohue as a whole fails to so anticipate. Applicant also respectfully submits that the Office fails to show how Donohue and Banzhof, alone or in combination, teach or suggest this claim. Namely, the Office fails to show how Donohue and Banzhof disclose, teach, or suggest, “means for receiving, *at a scan/patch server*, a binary signature and a security patch”, “means for scanning, *from the scan/patch server*, a client computer for a vulnerable file associated with the binary signature”, and “means for fixing, *from the scan/patch server*, the vulnerable file *on the client computer*”, as recited in Applicant’s claim. (emphasis added).

For at least these reasons, Applicant respectfully submits that this claim stands allowable.

Claim 25 recites a computer having a tangible component and comprising (emphasis added):

- binary information;
- a storage medium configured to retain the binary information;
- a scan module configured to receive a binary signature from a server and scan the binary information on the computer for the binary signature; and
- *a patch module configured to request a security patch from a server and install the security patch from the server if the binary signature is found in the binary information on the computer.*

In making out a rejection of this claim, the Office states that Donohue anticipates and/or that Donohue and Banzhof render the claim obvious. To do so, the Office uses reasoning similar to that discussed above in regards to claim 13.

Thus, for at least the reasons discussed above in regards to claim 13, Applicant respectfully submits that the Office fails to show how Donohue and Banzhof, alone or in combination, teach or suggest this claim. Namely, the Office fails to show how Donohue or Banzhof teach or suggest “a patch module configured to request a security patch from a server and install the security patch from the server if the binary signature is found in the binary information on the computer”, as recited in Applicant’s claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, Applicant respectfully submits that this claim stands allowable.

Claim 27 depends from claim 25 and, as such, the remarks made above in regards to claim 25 apply equally to this claim. The rejections of this claim is also improper as failing to show how the references of record teach or suggest, either singly or in combination, this claim’s own recited features in combination with those recited in claim 25.

Claim 28 recites a computer having a tangible component and comprising (emphasis added):

- binary files;
- a storage medium configured to retain the binary files;
- a binary signature; and
- a security patch module configured to receive the binary signature from a server and to scan the binary files on the computer in search of the binary signature;
- a binary file that includes the binary signature; and
- a security patch;
- *wherein the security patch module is further configured to request the security patch from the server upon locating the binary signature within the binary file, and to apply the*

security patch to the binary file that includes the binary signature.

In making out a rejection of this claim, the Office states that Donohue anticipates and/or that Donohue and Banzhof render the claim obvious. To do so, the Office uses reasoning similar to that discussed above in regards to claim 1. Thus, for at least the reasons discussed above in regards to claim 1, Applicant respectfully submits that the Office fails to show how Donohue and Banzhof, alone or in combination, teach or suggest this claim. Namely, the Office fails to show how Donohue or Banzhof teach or suggest “security patch module [that] is [] configured to request the security patch from the server upon locating the binary signature within the binary file”, as recited in Applicant’s claim. Instead, Donohue at most has been shown to describe retrieving and automatically installing updates to a computer.

For at least this reason, Applicant respectfully submits that this claim stands allowable.

Claim 30 recites a distribution server having a tangible component and comprising (emphasis added):

- a database embodied as a computer-readable storage medium; and
- *a distribution module configured to* receive a binary signature and a security patch, store the binary signature and the security patch in the database, and *distribute the binary signature and the security patch to a plurality of servers.*

In making out a rejection of this claim, the Office states that Donohue anticipates and/or that Donohue and Banzhof render the claim obvious. Applicant respectfully submits, however, that the Office fails to show how Donohue and

Banzhof, alone or in combination, teach or suggest this claim for at least the reasons discussed above in regards to claim 8. Namely, the Office fails to show how Donohue or Banzhof teach or suggest “a distribution module configured to...distribute the binary signature and the security patch *to a plurality of servers*”, as recited in Applicant’s claim. (emphasis added).

For at least this reason, this claim stands allowable.

Claim 31 depends from claim 30 and, as such, the remarks made above in regards to claim 30 apply equally to this claim. The rejections of this claim is also improper as failing to show how the references of record teach or suggest, either singly or in combination, this claim’s own recited features in combination with those recited in claim 30.

Claim 32 recites a server having a tangible component and comprising:

- a binary signature associated with a security vulnerability in a binary file;
- a security patch configured to fix the security vulnerability in the binary file;
- a database embodied as a storage medium and configured to store the binary signature and the security patch;
- a scan module configured to scan, from the server, binary files on a client computer for the binary signature and to update, from the server, the binary file on the client computer with the security patch if the binary signature is found, wherein the client computer is remote from the server.

In making out a rejection of this claim, the Office states that Donohue anticipates and/or that Donohue and Banzhof render the claim obvious. To do so, the Office uses reasoning similar to that discussed above in regards to claim 11. Thus, for at least the reasons discussed above in regards to claim 11, Applicant respectfully submits that Donohue does not anticipate this claim. Applicant also

respectfully submits that the Office fails to show how the combination of Donohue and Banzhof teach each element of this claim. For instance, Applicant respectfully submits that the Office fails to show how the references teach or suggest “a scan module configured to scan, *from the server*, binary files *on a client computer* for the binary signature and to update, *from the server*, the binary file *on the client computer* with the security patch if the binary signature is found, *wherein the client computer is remote from the server*”, as recited in Applicant’s claim. (emphasis added).

For at least this reason, Applicant respectfully submits that this claim stands allowable.

Claim 33 depends from claim 32 and, as such, the remarks made above in regards to claim 32 apply equally to this claim. The rejections of this claim is also improper as failing to show how the references of record teach or suggest, either singly or in combination, this claim’s own recited features in combination with those recited in claim 32.

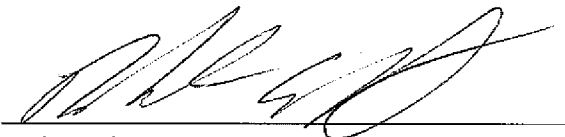
Conclusion

All of the claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 09/14/2007

By: _____


Robert G. Hartman
Reg. No. 58,970
(509) 324-9256 ext 265